BRIGHT IDEAS FOR MAKING CYBER STICK

govloop

A GOVLOOP GUIDE

INTRODUCTION

The hybrid cloud. Cloud-native operations. Digital services. Edge computing. With the rapid evolution of the government enterprise, agencies need to design, implement and maintain cybersecurity programs that are sophisticated enough to protect today's networks and data management.

And an agency's entire workforce must follow those plans, not just the tech-savvy IT staff who understand the intricacies of encryption and other cyber tools, for instance.

In this guide, we discuss the practices and processes that enable organizations to develop a cyber-aware culture with well-trained employees from diverse backgrounds.

We explain how to ditch cyber jargon in favor of plain language that most people can understand. And we highlight opportunities for cyber information sharing and success measurements, and incentives for following cyber standards.

We also share wisdom from government and industry experts, who speak from their personal experiences.

No one is excused from helping to protect their agency's networks, data and digital services.

It's a responsibility we all share.

CONTENTS

THE BASICS

ESSENTIAL ELEMENTS OF A CULTURE OF CYBER-READINESS

Source: Cybersecurity & Infrastructure Security Agency (CISA)

YOURSELF
(THE LEADER)

Drive cybersecurity strategy, investment and culture

YOUR SURROUNDINGS
(THE DIGITAL WORKSPACE)

Ensure only those who belong have access

YOUR STAFF
(THE USERS)

Develop security awareness and vigilance

YOUR DATA
(WHAT THE BUSINESS IS BUILT ON)

Make backups and avoid the loss of critical information

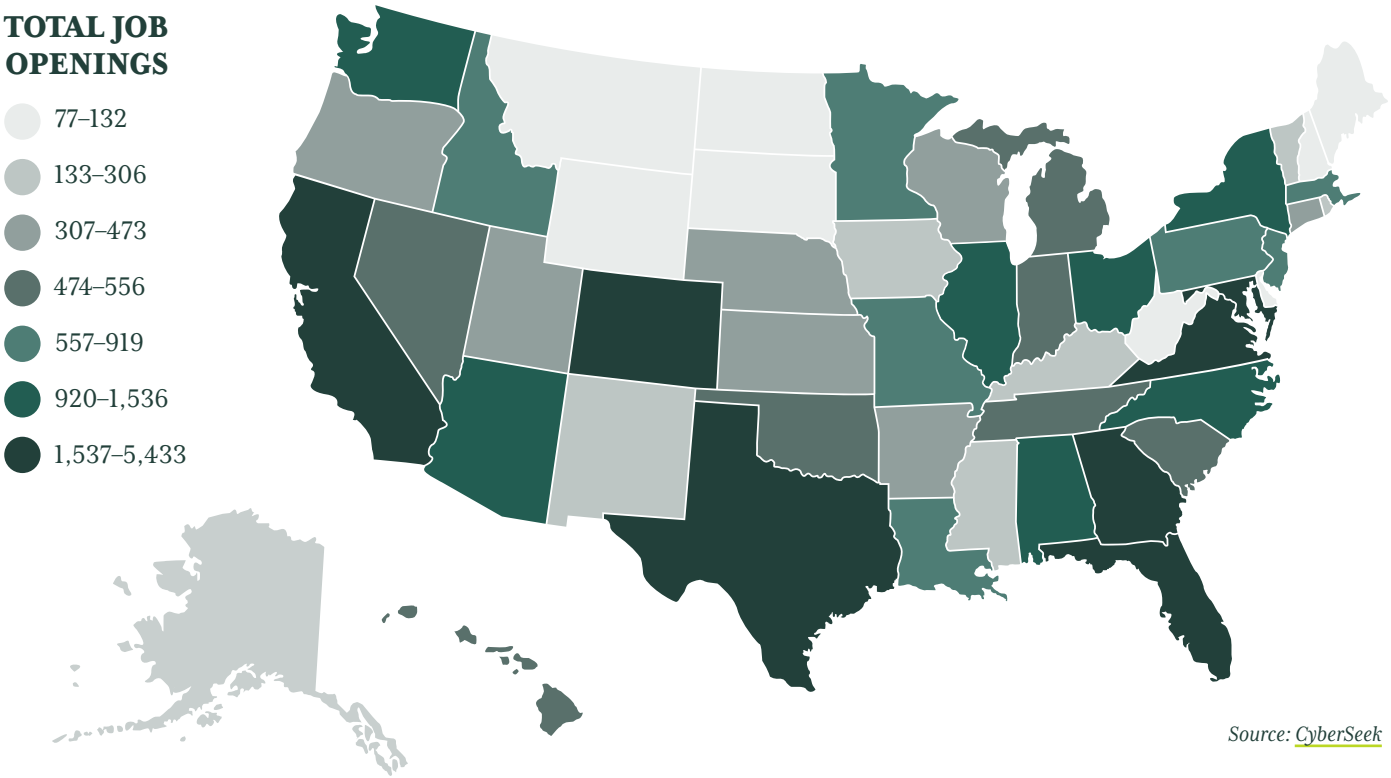
YOUR SYSTEMS
(WHAT MAKES YOU OPERATIONAL)

Protect critical assets and applications

YOUR CRISIS RESPONSE

Limit damage and quicken restoration of normal operations

STATE-BY-STATE CYBERSECURITY JOB SHORTAGES



Source: CyberSeek

TOP 5 BARRIERS STATES FACE WHEN ADDRESSING CYBERSECURITY CHALLENGES

2020	2022
#1 **Lack of sufficient cybersecurity budget** (46%)	#1 **Legacy infrastructure and solutions to support emerging threats** (52%)
#2 **Inadequate cybersecurity staffing** (42%)	#2 **Inadequate availability of cybersecurity professionals** (50%)
#3 **Legacy infrastructure and solutions to support emerging threats** (34%)	#3 **Inadequate cybersecurity staffing** (46%)
#4 **Inadequate availability of cybersecurity professionals** (28%)	#4 **Decentralized IT and security infrastructure and operations** (38%)
#5 **Lack of dedicated cybersecurity budget** (28%)	#5 **Increasing sophistication of threats** (29%)

Source: 2022 Deloitte-NASCIO Cybersecurity Study & 2020 Deloitte-NASCIO Cybersecurity Study

13 COMMON TYPES OF CYBERATTACKS

Malware attack: An umbrella term that refers to a hostile or intrusive program or file designed to exploit devices to the benefit of the attacker

Password attack: Obtaining someone's password in order to bypass security controls and access critical data and systems

Ransomware: A program designed to encrypt a victim's files and then demand a ransom in order to receive the decryption key

Man-in-the-middle attack: When attackers secretly intercept and relay messages between two parties who believe they are communicating directly with each other

Phishing: When an attacker masquerades as a reputable entity to distribute malicious links or attachments designed to trick someone into handing over valuable information

URL interpretation/URL poisoning: When hackers modify a URL — the unique identifier that tells a web browser (e.g., Google) where to find something on the internet — in order to access information or resources they shouldn't be able to

SQL injection attack: A malicious request to create, modify or delete data stored in a database, as well as read and extract intellectual property, customers' personal information, administrative credentials or private business details

Cross-site scripting: When an untrusted source is allowed to inject its own code into a web application and that malicious code is included in dynamic content delivered to a victim's browser

Distributed denial-of-service: When multiple compromised computer systems attack a server, website or other network resource and flood it with incoming messages and connection requests. The targeted system slows or crashes, denying service to legitimate users or systems.

DNS spoofing: When hackers manipulate the Domain Name System (DNS) that connects human-readable domain names to their corresponding IP addresses. Victims are directed to a hacker-controlled website instead of the legitimate one.

Botnet: A collection of internet-connected computers and devices that are infected and controlled remotely by cybercriminals

Watering hole attack: When attackers embed malicious code in a legitimate but insecure website that targeted users often visit, and each time someone visits the site, the code automatically infects their device

Insider threat: When people who have legitimate access to an organization's systems, and often have an in-depth knowledge of its cyber defenses, gain access to restricted resources to make system configuration changes, install malware or cause a data breach

THE JOURNEY

Like many things in life, effective cybersecurity is a process. It begins by fostering a culture in which people are aware of cyber hazards and willing to act against them, and it includes thoughtful communication that speaks to different audiences in language they understand.

It means stepping back and assessing what vulnerabilities remain, and for organizations slow to adopt cyber programs, it means compelling them to do so.

In the following pages, we take you on that journey of cyber protection, to help you and your agency develop a cyber program that matters.

GET A LITTLE CULTURE

TURN YOUR 'WEAKEST LINK' INTO A 'HUMAN FIREWALL'

It's typical to think of the workforce as cybersecurity's weakest link. That makes sense: According to a recent report, 82% of breaches across all industries involved human factors — stolen credentials, phishing, misuse or simple error. Most attacks target employees as the easiest route to gaining access. Companies, and agencies, often rely on technology to prevent incursions. While you need to keep malware blockers and other technology up to date, tech alone can't solve the problem.

An alternative approach transforms users into "a human firewall." But it takes more than a slideshow once a year. You need to establish — and maintain — the attitude that everyone is responsible for the safety of your systems and data, and then give them the right training and tools. **Create a culture of cybersecurity, and you can turn your weakest link into your best defense.**

THE SCOPE OF THE PROBLEM

In 2021, 2,792 incidents compromised government data, and 537 of them resulted in confirmed disclosure of data.

Although system intrusion, usually by well-organized cybercrime networks or state actors, has become much more frequent in the past two years, mistakes such as falling for a phishing attack, misconfiguring resources, sending data to the wrong recipient and losing devices account for most employee-caused breaches.

As we've learned in other spheres, often the way to reduce mistakes is not so much to change the people as to change the system. That's where culture comes into play.

MIT's Sloan School of Management describes a cybersecurity culture as one that "tasks every member of an organization with embracing attitudes and beliefs that drive secure behaviors." CISA's Cyber Essentials Starter Kit says it's one where staff "must have — and continuously grow — the skills to practice and maintain readiness against cybersecurity risks."

A cybersecurity culture builds on basic training that teaches cybersecurity concepts, terminology and best practices for employees. Make internal and external training resources available. Require regular refreshers, and encourage participation in campaigns such as National Cybersecurity Awareness Month. And don't expect people to do it on their own time.

But that's just the beginning.

TRAINING IS (ONLY) A STARTING POINT

Ongoing awareness starts from the top. To foster a true culture, according to MIT, leaders must commit to changing people's values, attitudes and beliefs about cybersecurity at every organizational level, and make it clear that cybersecurity is intrinsic to the agency mission. For example, start every meeting with a cybersecurity story.

Keep employees up to date by circulating information about trends in phishing, scams and email hijacking, and include them in regular training. Use real reported events to demonstrate current threats, and make sure everyone knows how to recognize and report them.

MODELS AND INCENTIVES

Have clear guidelines. For a culture to stick, people need to know what's expected of them. Written guidelines and policies should lay that out clearly. With those in place, you can apply incentives — both positive and negative — as reinforcement.

Use incentives and penalties. Recognition is surprisingly effective as a reward for getting it right and shows everyone that it matters. Other awards as appropriate could include gift cards or even time off. For getting it wrong, a graduated system starting with targeted training and progressing to loss of privileges, or even firing for repeated recklessness, might be necessary. Be sure to recognize cyber awareness in performance reviews.

And finally, make it fun. CISA and the Pacific Northwest National Laboratory are developing downloadable cybersecurity training games that feature simulated threats and responses in the context of typical computer games — quests, knights, ninjas. Winning depends on understanding cyberattacks, defenses and the role each person plays in protecting your resources. And what better way to reinforce your culture of cybersecurity?

DIVERSIFY THE WORKFORCE

INCLUSIVE TRAINING OPENS DOORS

*An interview with **Reinier Moquete**, Founder and CEO, CyberWarrior.com*

With more than 700,000 open cybersecurity positions in the United States, talent will not come from a single, well-positioned demographic.

"Cybersecurity careers represent a tremendous opportunity for those who, historically, have been on the economic sideline," said Reinier Moquete, Founder and CEO of CyberWarrior.com.

Moquete, who has held workforce development roles in two state administrations, leads CyberWarrior's rigorous six-month career-changer program. He also heads the nonprofit side that introduces cybersecurity to high schoolers, many from underserved and immigrant communities.

CHALLENGE

Diversified talent makes the industry stronger and more versatile, but the training programs themselves must be responsive to diverse needs, not one-size-fits-all.

For instance, many aspiring cyber professionals already work full time and are parents of young children. Their lives come with scheduling challenges, plus other accessibility or language challenges. They may have varying educational histories or different learning styles, which call for a continuum of support.

Traditional formats and rigid schedules cannot meet the needs of a wide variety of learners.

SOLUTION

Moquete believes that successful training for cybersecurity means being aware of inclusivity practices and demonstrating respect for people's lived experiences.

"At times, we forget that the individual is quite unique," Moquete said. "My life experiences vs. your life experiences make us different in the way that we learn, in the way that we approach problems and in the way that we engage with the workforce."

He believes that professionals grow through training that considers circumstance and asks, "How do we give you the attention and resources you need to be successful?"

A fully virtual learning environment, after-hours teaching assistance, Spanish language capabilities, flexibility and holistic assignments are a few of his tools. CyberWarrior also partners with organizations that assist with housing, food insecurity and childcare needs, so that students are better able to learn.

At almost every CyberWarrior session, there is at least one student holding a child or managing a home responsibility. And those students can be at the top of the class as easily as anyone else.

OUTCOME

CyberWarrior has made a dramatic impact on individual lives.

For instance, a first-generation Latino father worked two jobs to make a meager living and had no advancement opportunities. After six months of training, he became a network operations analyst.

A young Black woman held several jobs that didn't give her options to grow professionally. She received two job offers after completing the CyberWarrior program and became an associate security analyst.

"It's transformational," said Moquete. "From the start, she found her passion. She had zero related experience, but she worked very hard and earned three certifications."

Supportive, inclusive training, he said, is the key to filling the cyber workforce and changing the career trajectory of thousands of professionals.

LOOK FOR TALENT UPSTREAM

GEORGIA REDEFINES THE 'PERFECT' EMPLOYEE

*An interview with **David Allen**, former CISO, Georgia Technology Authority*

When David Allen began his role as Chief Information Security Officer (CISO) at the Georgia Technology Authority (GTA) in 2019, he knew he had a job in front of him. (He left for a private-sector job in October 2022.)

Competition for new employees was intense, but one of his top priorities was to increase the cyber workforce. The state's technology and IT enterprise management required it.

"That's something I attacked immediately," Allen said, aware that if agencies were short-staffed in cyber, that could hinder or even disrupt operations.

CHALLENGE

Allen began by looking at the open positions in his agency. He found that many, even entry-level jobs, required a four-year college degree.

He realized his agency had been seeking what some people think are perfect employees: highly educated, skilled in targeted areas and interested in working at a state agency. But that was too tall of an order, he believed, especially since GTA couldn't offer the high salaries available in the private sector.

How would he even begin to find interested and qualified candidates? And if they took the jobs, how long would they stay, really?

SOLUTION

Allen ushered in a new era, with positions calling for a high school diploma and a 12-month certification. Across Georgia agencies, he initiated pathways to cyber internships and employment for people without college degrees.

Regarding recruiting, Allen said that an agency should prioritize finding someone with the potential to develop skills and assume leadership, not just filling the position.

"I'm looking for that dynamic talent," he said. "I think it's out there, if you take the time to identify those new work streams."

The other part of his strategy was to invest in training.

"I have a military background, so I'm a big believer in cross-training and mentoring," Allen said. "The No. 1 job at my level is to prepare the next generation."

Even if new employees are learning on the job, he believes in the value they offer the agency and in the benefits for them personally.

OUTCOME

Allen's commitment to on-the-job training and mentorship set him apart when recruiting and hiring employees.

While CISO, he also taught at Georgia State University, which gave him the opportunity to connect with young, soon-to-be professionals. He brought his knowledge of their lives and abilities into his GTA recruiting strategy, always keeping mentoring and individual potential front of mind.

During his tenure, he built the youngest and most diverse cyber team at GTA.

"We build their trust and their confidence, and then let them go out and do the job," he said. "I've had many mentors over the years who have done that same thing for me. So, I try to carry that forward with my own people."

A PATH TO CYBER PROTECTION

Alcatel·Lucent Enterprise

*An interview with **Vincent Lomba**, Chief Technical Security Officer, Alcatel-Lucent Enterprise*

Government relies on data to make difficult decisions, and one data point is of significant concern to cybersecurity experts, said Vincent Lomba at Alcatel-Lucent Enterprise: Since the beginning of this year, the number of cyber vulnerabilities has doubled.

"The question is not will you be attacked, but what will be the consequence," Lomba said.

He believes that staff should know and understand an agency's cybersecurity strategy, with communications sent to them regularly. It also should be tested — in other words, an organization should conduct live simulations, perhaps without giving staff advanced knowledge of the exercise.

But there's one big challenge: financing.

ALLOCATING MONEY

Funding a cybersecurity program is difficult because it does not have a simple return on investment, Lomba said. "It's all about awareness at each and every level, especially at the executive level, to convince them that there is something to address [and] there is some money to invest," he said. They need to balance cost and protection.

Agencies don't have to guess about effective strategies for preventing cyber breaches. According to Lomba, cybersecurity insurers, which help organizations reduce their liability and financial exposure following a cyber breach, base their pricing and coverage decisions on probabilities and other statistics that agencies also can use.

SPEAKING IN PLAIN LANGUAGE

Cybersecurity jargon can be unintelligible to non-IT agency employees. **That's why using plain, simple language can make the difference between convincing leaders to fund cyber initiatives and allowing them to disregard cyber threats**, Lomba explained.

When talking about security measures, he said to focus on the basics: Let officials know that the agency is at risk and what the consequences are, and avoid "very complex, IT-guy" words.

FOLLOWING BEST PRACTICES

What guidance does Lomba offer for agencies contemplating cyber reforms? He encourages organizations to have dedicated, skilled people to manage their cybersecurity programs, and he urges agencies to ensure the cyber protection of the third parties with which they deal. In other words, make sure that everyone in the supply chain is protected, so their cyber vulnerabilities don't affect you.

Lomba also believes that organizations should consider cybersecurity options early on when buying new technology. Weighing only price and potential features is shortsighted, he said.

Alcatel-Lucent provides agencies with customized networking, communications and cloud solutions that help organizations follow these best practices. The firm accompanies agencies in their cybersecurity journeys and offers consistent support throughout the product's lifetime, Lomba said.

Sometimes the goal of cyber protection is to shield consumer data and prevent financial loss. But Lomba said sometimes the consequences of a data breach are more profound — for instance, when it would expose the names of personnel whose lives would be at risk.

Agencies must consider several fundamental questions, he said: "What is the importance of cybersecurity for you, and why do you want to put that into action? Is it just to be compliant with law, or is it also for something much more important than that?"

"The question is not will you be attacked, but **what will be the consequence.**"

TALK IN PLAIN LANGUAGE

MARICOPA COUNTY KNOWS ITS AUDIENCES

*An interview with **Lester Godsey**, Chief Information Security and Privacy Officer, Maricopa County, Arizona*

Maricopa County is the fourth most populous county in the nation, sprawled across south-central Arizona and home to more than half of the state's residents. It encompasses 9,224 square miles, including the state capital, 24 cities and towns, and several unincorporated entities.

Protecting the county's IT infrastructure from internal and external threats is profoundly important, and Lester Godsey, the county's Chief Information Security and Privacy Officer, knows that using simple, clear language is among his most important safeguards.

CHALLENGES

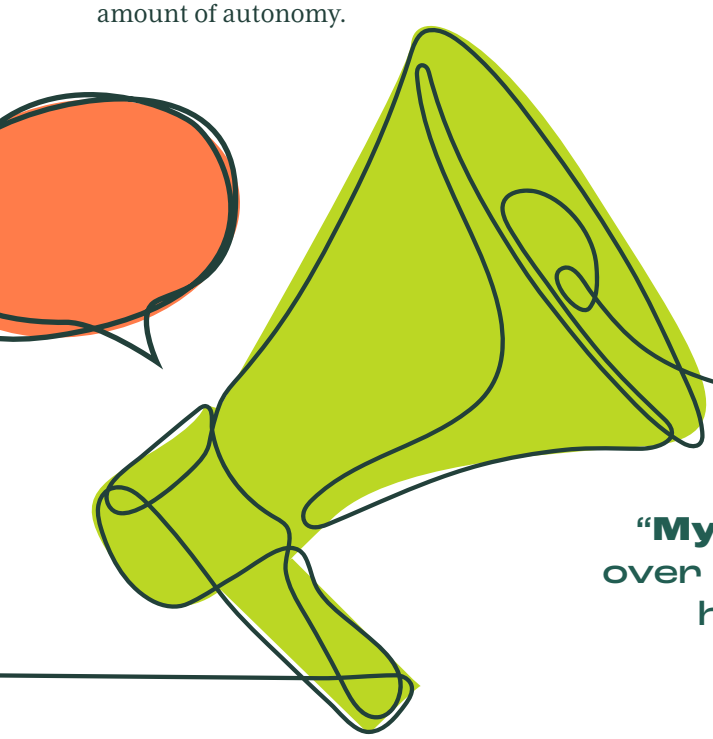
Agency IT professionals face a fundamental challenge: They need officials, politicians and agency staff to embrace — and perhaps fund — risk prevention measures that can save the organization time, money and reputation, but the audiences often have little tech acumen.

Further complicating matters is the fact that governments have multiple departments with different IT needs and sensitivities. In Maricopa's case, there are 56 departments, including eight run by political appointees with a fair amount of autonomy.

"My job is to protect the organization, and over the years, that definition of protection has extended to brand and trust of the organization as well," Godsey said.

"I can't afford to just focus on technology. I have to understand how our sheriff's office operates and what their unique constraints and requirements are vs. that of the court vs. that of animal care and control vs. that of public health," he said. "Technology always gets a spotlight," but communication is just as important.

The last few years in Maricopa County have been a stark reminder that government should prepare for the unexpected. Cybersecurity teams should, and often do, understand existing and potential risks and develop strategies to tackle them — but convincing people to appreciate and guard against those risks is a different matter.



"**My job is to protect the organization**, and over the years, that definition of protection has extended to brand and trust of the organization as well."

SOLUTION

Godsey defines "plain language" as "language that's used and is understandable by the widest audience, or the audience at the time." This means avoiding acronyms or industry jargon and putting information in context, making it relevant to the people you're approaching.

"If you can couch things in terms of risk, that's something that conceptually everybody understands," he explained. "Now, risk could be measured by a variety of different things, right? It's not just loss of money [or] loss of services. What we're finding that resonates with our elected officials is loss of trust by the public. Reputational impact is really what resonates."

For county departments that typically enjoy a certain degree of political independence, Godsey works to ensure a uniform, enterprisewide approach to cybersecurity by stressing cyber threats' apolitical nature. He tells department officials that "the bad guys don't care about [political sovereignty]. They're just looking for the path of least resistance, and once they get in, we're all at risk, and so it behooves all of us to be on the same page."

To entice county officials to participate in a tabletop exercise to help prepare for 2022 election threats, Godsey's team phrased the invitation simply, explaining the potential fallout from a cyber breach. "We had a packed house, and the feedback we got was really positive," he said.

Because department staff often disregard cybersecurity outreach from management, Godsey's team developed another effective plain-language communication tool: a "cybersecurity cadre program," in which line staff organizationwide "help spread the gospel of cybersecurity" to their colleagues, "people who don't know who that Lester guy is," he said.

OUTCOME

An effective cybersecurity program relies on basic marketing skills, and Godsey sees himself, in part, as a salesperson, telling the right stories to the right audiences.

The approach has "really paid dividends in terms of awareness and support for information security. … That's really bought us a lot of internal credit, and information security's really viewed highly within Maricopa County in terms of the services we provide and how we go about doing it," Godsey noted. "It's made my job subsequently easier, whether [I'm] requesting funding for initiatives or getting support within other departments for things we're trying to accomplish."

SHARE SO OTHERS MIGHT LEARN

NORTH CAROLINA MAKES CYBER A WHOLE-OF-STATE AFFAIR

*Insights from **James Weaver**, Secretary of Technology and Chief Information Officer, state of North Carolina*

In March 2022, the FBI issued a warning that ransomware attacks were straining local governments and public services. This was not news. Nationwide, numerous city and county offices, police departments, schools, and other local agencies had reported suffering data breaches and service disruptions.

In North Carolina, state leaders recognized that such attacks are not just local problems with local ramifications. City and county offices and services interconnect with one another and with state agencies. They all have a vested interest in working together to improve their collective security.

CHALLENGE

The FBI said that most attacks targeted smaller municipalities and counties, given that they were likely to have resource and budget limitations. Being underfunded and understaffed and working with outdated systems "often put them in the position to pay ransoms simply to get the data back," the FBI noted.

"We've got to recognize that government entities don't all have the same capabilities," said James Weaver, Secretary of Technology and Chief Information Officer (CIO) for North Carolina, speaking during a recent GovLoop online training. "Even at the state level, we have agencies with varying capabilities."

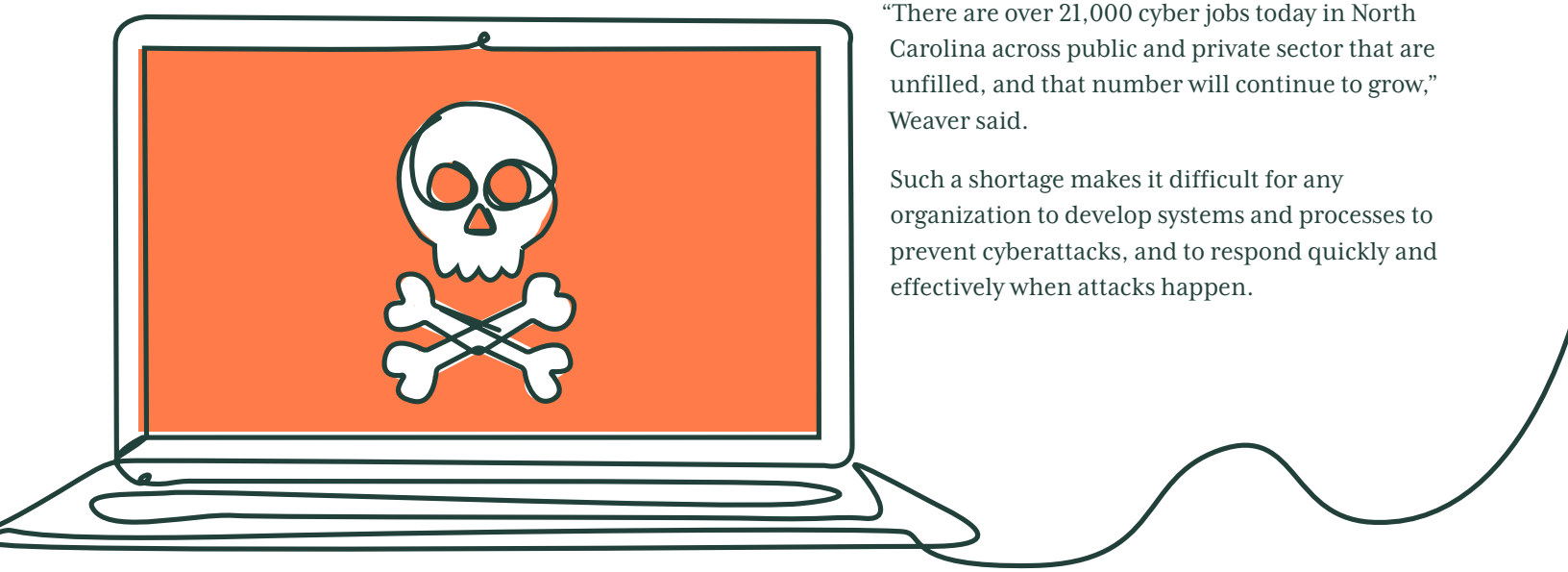
The North Carolina Department of Commerce annually ranks the state's 100 counties based on economic well-being and assigns each a tier designation. The 40 most economically distressed counties — Tier 1 — are the likeliest to struggle with cybersecurity.

"In some Tier 1 counties, the IT guy is probably also the person who is mowing the grass, who's doing three or four other things," Weaver said. "And in some cases, they're also running critical infrastructure systems."

But larger municipalities and counties are struggling to staff up, too; the competition for cyber experts is fierce.

"There are over 21,000 cyber jobs today in North Carolina across public and private sector that are unfilled, and that number will continue to grow," Weaver said.

Such a shortage makes it difficult for any organization to develop systems and processes to prevent cyberattacks, and to respond quickly and effectively when attacks happen.



SOLUTION

To address these challenges, North Carolina is taking a whole-of-state approach to cybersecurity. The initiative, which began in 2018, encompasses a wide range of entities, from state and local government and educational institutions to organizations managing critical infrastructure.

Every organization is doing its best to secure the data under its purview, to protect the state's citizens and businesses. A whole-of-state approach means "bringing all those resources together," Weaver said.

The initiative has three key components:

- The NC Information Sharing Analysis Center (NC-ISAC), which collects and analyzes emerging threats and cyber incidents
- Mandatory cyber incident reporting by all local government entities, with reports required within 24 hours of a confirmed attack
- The NC Joint Cybersecurity Task Force, a cross-government team that supports agencies dealing with an attack

With mandatory incident reporting, NC-ISAC can provide a comprehensive view of the cyber landscape statewide, which helps cyber experts understand and prepare for emerging and active threats.

Meanwhile, the joint task force brings the kind of cyber expertise that many individual agencies lack, including in advanced threat hunting and incident response. But just as important, they help agencies build their own expertise in preventing and responding to attacks.

OUTCOMES

Weaver makes clear that a whole-of-state approach does not mean a Big Brother approach. It hinges on giving local entities a voice in the process.

The task force includes representatives from the North Carolina Local Government Information Systems Association, an IT professional association that also manages an IT Strike Team that assists local agencies with emergency responses.

The association's involvement is not just for appearances, Weaver said. "If it's a local government-related incident, [the association] is driving the conversation. Everyone else is a partner [in the process]."

This is one of the guiding principles of a whole-of-state approach: Everyone is a stakeholder.

"At the end of the day, it's one team, one fight," Weaver said.

"At the end of the day, it's one team, one fight."

GET A REALITY CHECK

COUNTIES ASSESS THEIR CYBER READINESS

An interview with ***Rita Reynolds****, CIO, National Association of Counties*

In spring 2022, the National Association of Counties (NACo) partnered with SecurityScorecard, a cybersecurity ratings company, to help county governments monitor and improve cybersecurity risk. Such assessments were not really necessary as recently as 15 years ago, said Rita Reynolds, NACo's CIO, but the landscape is totally different today. From the types of attacks that take place, constantly increasing vulnerabilities, and growing automation and digitization, it's crucial that governments monitor their security.

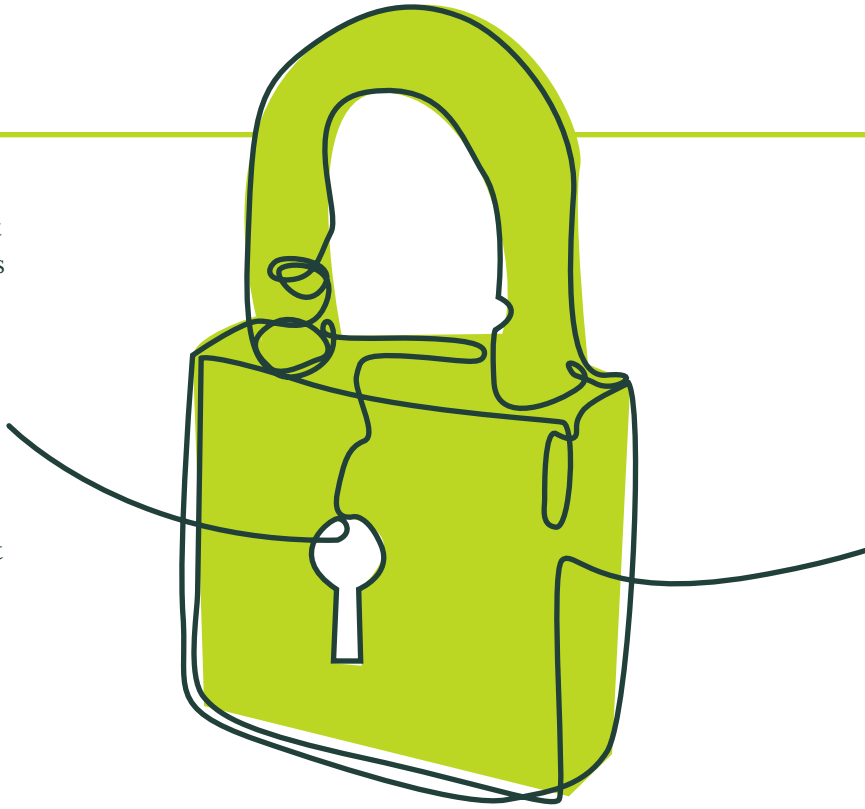
CHALLENGE

Assessments may be necessary, but they're not easy. For one, they can be pricey. A midsize organization can expect to pay $15,000 to $40,000, but the level of expertise makes it worthwhile, Reynolds said. They know to look for things that are common across the board, which gives them a starting place, and they dig down from there.

"You of course can do an internal assessment, but it's always better to have an external assessment done to ask all those questions to check your systems," Reynolds said. "We have got myriad different systems with different configurations. [You want to know:] Is everything set, right? Do you have permission set correctly? Are you exposed because there's known vulnerabilities in the software that you're using and you haven't applied a patch? All of that comes out from an assessment of your internal system."

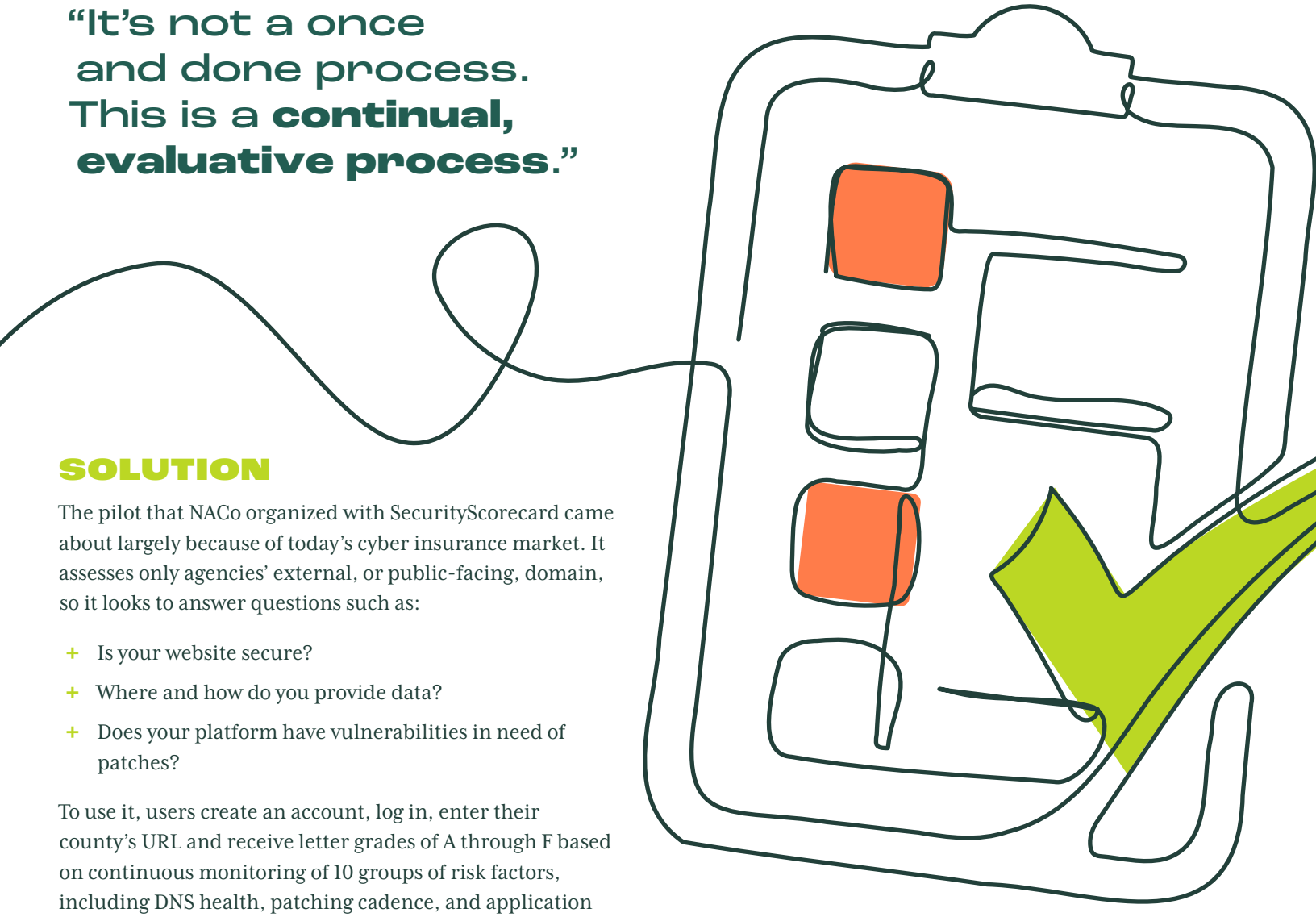
Another downside of county agencies handling assessments themselves is that they can be another drag on what's already faltering staff resources in many places.

Reynolds didn't have a percentage of how many of the country's 3,000-plus counties conduct cybersecurity assessments, but she said many do, at least at some point. "It's not every year. Some counties can't budget for the $30,000 or $40,000 or $50,000 for the assessment or the penetration test, so they might do it every other year," she said.



But many cyber insurance companies now require these assessments before they'll provide coverage, which government organizations increasingly need. Premiums have doubled and even quadrupled for some counties, and requirement questionnaires demand details on what cybersecurity agencies have in place. Assessments can answer those questions.

> "It's not a once and done process. This is a **continual, evaluative process.**"



SOLUTION

The pilot that NACo organized with SecurityScorecard came about largely because of today's cyber insurance market. It assesses only agencies' external, or public-facing, domain, so it looks to answer questions such as:

- Is your website secure?
- Where and how do you provide data?
- Does your platform have vulnerabilities in need of patches?

To use it, users create an account, log in, enter their county's URL and receive letter grades of A through F based on continuous monitoring of 10 groups of risk factors, including DNS health, patching cadence, and application and endpoint security. Through a dashboard, counties can drill down to see why they earned the grade they did — and begin work to bring it up.

"It could be a type of patch that needs to be applied, and I just didn't know it, but as soon as I do that, then the finding goes away," Reynolds said. "I can set an alert that says, 'Every time my score goes down, send me an email,' because I want to know if my score drops."

The two-month spring pilot was open to the 900 county IT leaders who are part of NACo's County Tech Xchange, an online portal that provides technology infrastructure resources. Thirty-eight counties actively participated in the test, many of which have continued to use the scorecard, although some counties use the platform but were not part of the pilot, she said.

OUTCOME

"We saw an improvement in the overall scores," Reynolds said. "We actually had a number of counties that were in the D range and the C range [and] that number went down. And those in the B range, the score went up. The score of A actually went down a little bit, but that's going to happen; you're going to go back and forth between A and B.

"That's the other thing that the pilot showed, it's not a once and done process," she continued. "This is a continual, evaluative process."

What do the improvements translate to? Eight pilot participants who increased from D to C reduced their risk of cyber breach by 140%, she said.

THE STICK NOT WORKING? TRY A CARROT

A CONNECTICUT LAW OFFERS A TEMPTING INCENTIVE

An interview with ***Jeffrey Brown****, CISO, state of Connecticut*

The Connecticut General Assembly enacted Public Act 21-119 in 2021 to encourage organizations to adopt standard cybersecurity frameworks in exchange for legal immunity should they be sued for a cyber breach. In other words, as long as they can prove current, reasonable cybersecurity controls were in place, "the Superior Court shall not assess punitive damages."

CHALLENGE

Espousing the adoption of cybersecurity control is easy when it comes to regulated industries because governments can mandate their use, said Jeffrey Brown, Connecticut's CISO. For general private companies, however, it's voluntary and there's no real mechanism to enforce implementation.

That opens organizations to risk, including — perhaps especially — lawsuits should a cyber incident occur. Given the financial and reputational costs of breaches, the state wanted to incentivize organizations to put protections in place.

"When I look at cybercrime, it's one of the few things where the victim gets blamed: your security wasn't good enough, some people broke in. It's like a punishment for a crime you didn't commit," Brown said. "What we're trying to do in the state of Connecticut is really be more proactive and encouraging for people to adopt these best practices."

SOLUTION

"We really needed to codify something that could stand in a court of law and doing that through legislation really seemed to be the right message," Brown said.

The law, called "An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses," calls on organizations to follow the industry cyber standard that best suits their missions. As a result, it deliberately recognizes options, including the National Institute of Standards and Technology's special publications 800-171, 800-53 and 800-53a; the Federal Risk and Management Program's FedRAMP Security Assessment Framework; the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or the International Organization for Standardization and the International Electrotechnical Commission's 27000-series.

Additionally, the law requires conformity with the "current versions" of those standards, or a combination of them, although Brown said it's reasonable about allowing organizations time to implement updates. "If there's a brand-new version just released today, now everyone's out of compliance — it's not like that," he said.

OUTCOME

Brown said several companies have told him that they are interested in reducing their legal liabilities for a cyber breach. "That means that those companies are now doing improvements to their security, they're looking at adopting frameworks, so that is a tangible benefit," he said. After all, the more secure all agencies are, the more secure the government is.

Because the law is still new, it has not been proven in court yet, but he expects that it will. "Unfortunately, there's certainly ample opportunity for cyber breaches and [for] being able to get to something like this through court to see how it does," Brown added.

READING ROOM

+ Cybersecurity & Infrastructure Security Agency: Cyber Resource Hub
+ CISA Cyber Essentials Starter Kit: The Basics of Building a Culture of Cyber Readiness
+ CISA Insights: Cyber: Enhance Email & Web Security
+ National Governors Association: Resource Center for State Cybersecurity
+ National Association of Counties: Cybersecurity for Counties
+ Federal Virtual Training Environment: Free Online Cybersecurity Courses

GOVLOOP RESOURCES:

+ Guide: Why Zero Trust Matters at Work (and How to Foster It)
+ Article: Only You Can Prevent Ransomware
+ Article: How One State Advances Cyber Protection

CONCLUSION

It is easy to appreciate cybersecurity's basic premise — preventing hackers from getting inside your agency's systems and stealing data. But protecting your organization requires more than the right technology, as important as that is.

In this guide, we took you on a journey. We started with the fundamentals of building a cyber-aware workforce and hiring talented and diverse staff. We showed why it's crucial to speak honestly and in plain language, share knowledge among agencies, and assess the success of your cyber programs. And, we offered a case study for encouraging cyber initiatives across all government agencies.

Cyber threats have become more frequent and complex. All organizations, including yours, must be prepared.

THANK YOU

Thank you to Akamai, Alcatel-Lucent Enterprises, Elastic, Dragos, Keeper Security, Palo Alto Networks and Red Hat for their support of this resource for public sector professionals.

ABOUT GOVLOOP

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector. For more information about this report, please reach out to info@govloop.com.

AUTHORS

Candace Thorson, Managing Editor
Lauren Walker, Senior Staff Writer
John Monroe, Director of Content
Susan Kirby-Smith, Senior Staff Writer
Stephanie Kanowitz, Contributing Writer

DESIGNER

Kaitlyn Baker, Senior Creative Manager